JDL Group

go for IT

Hackers are Using Malware to Generate Cryptocurrencies

February 28, 2018

Cryptocurrencies enjoyed an incredible 2017 and are still unbelievably popular in 2018. Ever since Bitcoin's price skyrocketed throughout last year, cryptocurrencies have been a hot topic for news organizations and financial institutions alike. Some believe Bitcoin and other cryptocurrencies

such as Ethereum, Litecoin, and Monero are the currency of the future, while others believe they are just another get rich quick scheme.

Regardless of how you feel about cryptocurrencies, the fact is that the crypto industry largely operates without rules or regulations imposed by financial institutions or governments, at least for now. This has opened the door for hackers to use malware and malicious code to illegally generate cryptocurrency. Let's take a look at a few recent examples and what you can do to protect yourself.

Android Users Targeted for Cryptocurrency Mining

A new drive-by Monero crypto-mining campaign that targets Android users on their mobile devices has emerged. This campaign actually tricks victims into authorizing crypto-mining on their device. When potential victims navigate to a specific website, they are greeted by a fake message stating that their device is exhibiting "suspicious" activity. They are then prompted to solve a CAPTCHA using code w3FaSO5R. Once this code is inputted and the "continue" button is clicked, the android device begins the cryptocurrency mining process. This drains your device of all its energy in order to illegally mine the cryptocurrency Monero. Protect yourself from this campaign by always scanning your device regularly with an antivirus application and watching out for any unexpected jumps in your devices' CPU usage.

Coinhive Discovered in Google Play Apps

Coinhive, a deceptive cryptocurrency-mining script used to mine cryptocurrencies from unknowing victims has been discovered in 19 different Google Play Apps. As soon as a user opens one of these apps, Coinhive opens a WebView browser instance that begins the cypto-mining process. One of the infected apps has even been downloaded between 100,000 and 500,000 times! Check out this list of the malicious apps by

Sophos. If you have downloaded any of the malicious apps, immediately uninstall it and scan your device with an antivirus application.

US and UK Government Sites Infected

The BrowseAloud plugin, a TextHelp software that improves website accessibility for disabled users was recently the target of a supply-chain style attack from hackers. Over 4,000 websites were affected by this attack, including multiple US and UK government websites. The attack added cryptocurrency-mining script to the BrowseAloud plugin that used victims' CPUs to produce Monero illegally. All website owners should routinely examine their websites for any unusual changes, behavior, or JavaScript code.

Securing Your Devices Against Hackers

Hackers are always going to find new ways to use malware and ransomware for nefarious purposes, and the crypto craze is just the latest example of that. You and your business need a qualified IT security vendor to watch your back. Contact JDL Group today.

Additional Resources

https://publicwww.com/websites/browsealoud.com%2Fplus%2Fscripts%2Fba.js/
https://www.texthelp.com/en-gb/company/corporate-blog/february-2018/data-security-investigation-underway-at-texthelp/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-coinminer-and-other-malicious-cryptominers-tpna.pdf?la=en
https://blog.malwarebytes.com/threat-analysis/2018/02/drive-by-cryptomining-campaign-attracts-millions-of-android-users/

CONTACT US

200 CONNELL DRIVE, SUITE 1100
BERKELEY HEIGHTS, NJ 07922
SALES@JDLGRP.COM
TEL: 973.975.4018

Schedule a Call

Schedule a Consultation 973-975-4018